



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/548,257	04/12/2000	Rudolph Balaz	MS1-467US	6164

22801 7590 06/21/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

8

DATE MAILED: 06/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/548,257

Applicant(s)

BALAZ ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-56 is/are pending in the application.
- 4a) Of the above claim(s) 14-16 and 40-56 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9, 11-13, 17-25 and 31-39 is/are rejected.
- 7) ☒ Claim(s) 10, 26-30 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of claims 1-13 and 17-39 in Paper No. 7 is acknowledged.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on June 25, 2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,2,6-9,11,17-19,21,24,25,36, and 38 are rejected under 35

U.S.C. 102(e) as being anticipated by Mikurak, U.S. Patent 6,606,744.

As per claim 1, it is taught by Mikurak of a Registration Authority comprising a gateway that acts as a protocol converter that is coupled to receive messages from a

Art Unit: 2131

router targeting a certificate authority and to receive messages from the Certificate Authority targeting the router (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). The teachings of Mikurak disclose of sending messages to and from a Certificate Authority across a router using a gateway to convert protocols (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). It is interpreted by the examiner that the gateway converts messages received from the router in accordance with a first protocol and converts the messages received from the router to a second protocol, then communicates the converted messages and conversely, that the gateway converts the messages received from the Certificate Authority in accordance with the second protocol and convert the messages received from the certificate authority to the first protocol, then communicates the converted messages. Since it is disclosed by Mikurak that without the use of gateways to convert the protocols, the information (messages) would be incomprehensible upon arrival and gateways allow incompatible networks to communicate with one another (col. 67, lines 15-25) which indicates that messages are converted from a first protocol to a second protocol and from a second protocol to a first protocol so that the incompatible networks can communicate.

As per claim 2, it is shown in the teachings of Mikurak in Figure 120 that the Registration Authority (RA) is independent of the Certificate Authority (CA) since they are remotely located from one another.

As per claim 6, Mikurak discloses that a router is connected to a Certificate Authority as is shown in Figure 120. A certificate request (get certificate message) is passed to the Registration Authority (col. 275, lines 55-56).

As per claim 7, it is disclosed by Mikurak that a router is connected to a Certificate Authority and a Registration Authority as is shown in Figure 120. A certificate request (get certificate message) is passed to the Registration Authority (col. 275, lines 55-56). The Certificate Authority sends a response message in regards to the message received by the registration authority (col. 269, lines 58-63).

As per claim 8, it is disclosed by Mikurak that a router is connected to a Certificate Authority and a Registration Authority as is shown in Figure 120. It is interpreted by the examiner that the router is unaware that it is communicating with a Registration Authority rather than directly with the Certificate Authority because routers look at the destination address and sends the data to that location and is unaware of what particular device that resides at the destination location, but rather identifies that destination location by its destination address (col. 67, lines 26-36).

As per claim 9, Mikurak discloses that a router is connected to a Certificate Authority as is shown in Figure 120. It is also recited that the router maintains a transaction ID table that maps data packets (router transaction IDs) received from the router to data packets (Certificate Authority request IDs) received from the Certificate Authority (col. 67, lines 26-36 and col. 269, lines 58-63).

As per claims 17 and 18, it is disclosed by Mikurak of a computer readable medium (media) having computer software (program) stored thereon that when

executed by a processor, allow a Registration Authority comprising a gateway that acts as a protocol converter that is coupled to receive messages from a router (device) targeting a certificate authority and to receive messages from the Certificate Authority targeting the router (col. 51, lines 29-33, col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). The teachings of Mikurak disclose of sending (first, second, third, and fourth) messages/responses to and from a Certificate Authority across a router using a gateway to convert protocols (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). It is interpreted by the examiner that the gateway converts (first, second, third, and fourth) messages/responses received from the router in accordance with a first protocol and converts the messages/responses received from the router to a second protocol, then communicates the converted messages/responses and conversely, that the gateway converts the messages/responses received from the Certificate Authority in accordance with the second protocol and convert the messages received from the certificate authority to the first protocol, then communicates the converted messages/responses. Since it is disclosed by Mikurak that without the use of gateways to convert the protocols, the information (messages) would be incomprehensible upon arrival and gateways allow incompatible networks to communicate with one another (col. 67, lines 15-25) which indicates that messages/responses are converted from a first protocol to a second protocol and from a second protocol to a first protocol so that the incompatible networks can communicate.

As per claim 19, Mikurak recites of a (first) message comprising an enrollment request (message)(col. 303, lines 3-7).

As per claims 21,24, and 25, Mikurak teaches of a certificate that is issued (by a third message or CA pending response) and is included in a reply (fourth message) that is encrypted by use of SSL that includes a digital signature (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56).

As per claim 36, Mikurak recites of a (first) message comprising an enrollment request (message)(col. 303, lines 3-7). The teachings of Mikurak disclose of the use of signatures and encryption and use of the X.509 standard (col. 238, lines 1-15 and col. 264, lines 42-51). An enrollment (first) message is signed and encrypted by a sender (device) and is sent to a recipient, or RA, that decrypts the message and authenticates (verifies) the sender and then sends a request (second message) to a CA for a certificate (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56).

As per claim 38, Mikurak teaches of a generated certificate that is issued (extracted) and is included in a reply (fourth message) that is encrypted by use of SSL that includes a digital signature (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mikurak in view of Cisco System's Simple Certificate Enrollment Protocol, herein referred to as Cisco.

The teachings of Mikurak disclose of a Registration Authority comprising a gateway that acts as a protocol converter that is coupled to receive messages from a router targeting a certificate authority and to receive messages from the Certificate Authority targeting the router (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). The teachings of Mikurak disclose of sending messages to and from a Certificate Authority across a router using a gateway to convert protocols (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). Mikurak additionally recites of a message comprising an enrollment request (col. 303, lines 3-7). The teachings are silent in disclosing of the use protocols consisting of Simple Certificate Enrollment Protocol and Public-Key Cryptography Standards enrollment protocol. Cisco recites of both Simple Certificate Enrollment Protocol (SCEP) and Public-Key Cryptography Standards (PKCS) enrollment protocol (pg 1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply protocols that allow for certificate authority implementations.

Cisco recites of motivation benefits of these protocols by disclosing PKCS uses authenticated public keys that protects the identity information in the enrollment requests and certificates (pg 3, section 2.4) and the goal of SCEP is to support secure issuance of certificate to network devices in a scalable manner (pg 1, section 2.0). It is obvious that the teachings of Mikurak would have found the use to SCEP and PKCS to be crucial so that the identity information is an enrollment request and to issue certificates in a secure manner as is disclosed by Cisco.

7. Claims 5,20,22,23,31-35,37, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mikurak in view of Housley et al.

As per claim 5, the teachings of Mikurak recite of a computer readable medium (media) having computer software (program) stored thereon that when executed by a processor, allow a Registration Authority comprising a gateway that acts as a protocol converter that is coupled to receive messages from a router (device) targeting a certificate authority and to receive messages from the Certificate Authority targeting the router (col. 51, lines 29-33, col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). The teachings of Mikurak disclose of the use of signatures and encryption and use of the X.509 standard (col. 238, lines 1-15). The teachings are silent in disclosing that they conform to the network Working Group Request for Comments 2459 standard. The teachings of Housley et al disclose of the network Working Group Request for Comments 2459 standard (see page 1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply rules for use with X.509. Housley et al recites motivational

Art Unit: 2131

benefits of the use of network Working Group Request for Comments 2459 standard by disclosing that X.509 certificates are allowed to be used on the Internet and it defines a profile to promote the development of certificate management systems, interoperability determined by policy, and the development of application tools (pg 2, section 2). It is obvious that the teachings of Mikurak follow the network Working Group Request for Comments 2459 standard since it is used across the Internet and Housley et al offers a policy for use of X.509 certificates in this environment.

As per claim 20, the teachings of Mikurak recite of a computer readable medium (media) having computer software (program) stored thereon that when executed by a processor, allow a Registration Authority comprising a gateway that acts as a protocol converter that is coupled to receive messages from a router (device) targeting a certificate authority and to receive messages from the Certificate Authority targeting the router (col. 51, lines 29-33, col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). Mikurak additionally recites of a (first) message comprising an enrollment request (message)(col. 303, lines 3-7). The teachings of Mikurak disclose of the use of signatures and encryption and use of the X.509 standard (col. 238, lines 1-15 and col. 264, lines 42-51). An enrollment (first) message is signed and encrypted by a sender (device) and is sent to a recipient, or RA, that decrypts the message and authenticates (verifies) the sender and then sends a request (second message) to a CA for a certificate (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56). The teachings of Mikurak fail to disclose of using subject alternative name extensions in a certificate. It is taught by Housley et al of the X.509

standard that discloses the use of subject alternative name extensions in a certificate (pg 31, section 4.2.1.7). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply usage of subject alternative name extensions in a certificate. Housley et al recites motivation for use of subject alternative name extensions by disclosing additional identities are associated to the subject of the certificate than can include email addresses, DNS names, IP addresses, or URIs and because the subject alternative name extensions are definitively bounded to a public key, it has to be verified by a CA (pg 31, section 4.2.1.7). It is obvious that the teachings of Housley et al could be implemented in the teachings of Mikurak as a means to allow different identities to be associated with a subject of a certificate as is disclosed by Housley et al.

As per claims 22,23, and 39, Mikurak teaches of a certificate that is issued (by a third message) and is included in a reply (fourth message) that is encrypted by use of SSL that includes a digital signature (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56). The teachings of Mikurak disclose of the use of the X.509 standard (col. 238, lines 1-15). The teachings of Mikurak are silent in disclosing of the use of accessing sets/chains of certificates. It is disclosed by Housley et al in the X.509 standard that recites of accessing a chain (set) of certificates (pg 9, section 3.2). It would have been obvious to a person of ordinary skill in the art to have been motivated to apply sets of certificates based on the X.509 standard. Housley et al recites motivation for a chain (sets) of certificates by disclosing certification chains are required because a public key user is only initialized with a limited number of CA

assured public keys (pg 9, section 3.2). It is obvious that the teachings of Housley et al could be applied to the teachings of Mikurak as a means of limiting the number of CA public keys as is suggested by Housley et al.

As per claim 31, Mikurak teaches of sending (first) messages to a Registration Authority and of certification revocation (col. 273, lines 33-38), but fails to adequately disclose sending for a certificate revocation list. It is taught by Housley et al of issuing certificate revocation lists (pg 11, section 3.3). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have applied certificate revocation lists as a means of checking the validity of certificates. Housley et al discloses motivation for the use of certificate revocation lists by reciting in some instances, certificates may become invalid prior to expiration of the certificate, so the certificate needs to be revoked and the certificate revocation list identifies revoked certificates (pg 11, section 3.3). It is obvious that by listing certificate revocation lists, a certificate that has been revoked prior to expiration can be identified and not considered valid as is disclosed by Housley et al and the teachings of Mikurak would have identified the revoked certificate earlier rather than allow the revoked certificate to have been honored as valid.

As per claims 32 and 37, Mikurak recites of a (first) message comprising an enrollment request (message)(col. 303, lines 3-7). The teachings of Mikurak disclose of the use of signatures and encryption and use of the X.509 standard (col. 238, lines 1-15 and col. 264, lines 42-51). A (first) message is signed and encrypted by a sender (device) and is sent to a recipient, or RA, that decrypts the message and authenticates

(verifies) the sender and then sends a request (second message) to a CA for a certificate (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56). The teachings of Mikurak are silent in disclosing of the use of a certificate serial number. It is disclosed by Housley et al of serial numbers that are associated with certificates (pg 17 section 4.1.2.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply serial numbers to certificates. The motivational benefits of the use of certificate serial numbers is that it is a value that is unique for each certificate that is issued by a particular CA, whereby an example given by Housley et al is the issuer name and serial number uniquely identify a unique certificate (pg 17, section 4.1.2.2). It is obvious that the teachings of Mikurak use certificate serial numbers so that they can be uniquely identified as is disclosed by Housley et al.

As per claim 33, Mikurak teaches of a certificate that is issued (by a third message or CA pending response) and is included in a reply (fourth message) that is encrypted by use of SSL that includes a digital signature (col. 264, lines 42-61, col. 269, lines 47-63, col. 273, lines 23-38, and col. 275, lines 42-56). Housley et al is relied upon for the use of issuing certificate revocation lists contained (extracted from) within a certificate from public repository (distribution point)(pg 11, section 3.3). Please refer to the motivation as to why it is obvious to apply the teachings of Housley et al to Mikurak as is recited above.

As per claim 34, Housley et al teaches of issuing certificate revocation lists contained within a certificate from public repository (distribution point)(pg 11, section

3.3). The distribution point can be located on-line (located at a particular URL) to interoperability on the Internet (pg 12, section 3.3). Please refer to the motivation as to why it is obvious to apply the teachings of Housley et al to Mikurak as is recited above.

As per claim 35, Housley et al teaches of issuing certificate revocation lists contained within a certificate (obtained) from public repository (distribution point)(pg 11, section 3.3). Please refer to the motivation as to why it is obvious to apply the teachings of Housley et al to Mikurak as is recited above.

8. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mikurak in view of Li et al.

Mikurak discloses that a router is connected to a Certificate Authority as is shown in Figure 120. It is also recited that the router maintains a transaction ID table that maps data packets (router transaction IDs) received from the router to data packets (Certificate Authority request IDs) received from the Certificate Authority (col. 67, lines 26-36 and col. 269, lines 58-63). The teachings of Mikurak are silent in disclosing of the use of table that maintains a valid password for a router. It is disclosed by Li et al of passwords being used for authentication that are associated to routers (col. 11, lines 10-17). State information is recorded (by means of a table) that includes the authentication information (including passwords)(col. 13, lines 5-30). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply passwords so that routers can be authenticated. Li et al recites motivation for the use of this concept by reciting passwords are used to ensure that

routers get their information from a packet issued by a router within their group (col. 11, lines 12-14). The teachings of Mikurak would have found this beneficial to ensure that information passed between a Certificate Authority and Registration Authority by means of a router are received by the appropriate destination as is taught by Li et al.

9. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mikurak in view of An et al.

As per claim 12, the teachings of Mikurak disclose of a Registration Authority comprising a gateway that acts as a protocol converter that is coupled to receive messages from a router targeting a certificate authority and to receive messages from the Certificate Authority targeting the router (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). The teachings of Mikurak disclose of sending messages to and from a Certificate Authority across a router using a gateway to convert protocols (col. 67, lines 15-19,21-25; col. 269, lines 58-65; and as shown in Figure 120). The teachings of Mikurak are silent in disclosing of receiving a request for a certificate of the certificate authority and return a certificate of the registration authority. It is disclosed by An et al an RA sending a request to a CA for a certificate and returning the certificate to the RA (col. 12, lines 22-28). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply the sending of a certificate from a certificate authority to a registration authority. An et al recites motivation for the use of the concept by disclosing registration authorities determine whether an applicant is authorized to receive access secure services to

receive a certificate as issued by a certificate authority after approval by a registration authority (col. 2, lines 35-41). By allowing a registration authority to authorize a requesting party for a certificate authority, it is obvious that the teachings of Mikurak would have used this process in order determine if a certificate should be issued from a certificate authority and then passed to a registration authority prior to issuing it to a requesting party.

As per claim 13, An et al discloses of the registration authority being automated (col. 12, lines 24-28). The examiner is interpreting the automation as being a dynamically linked library since it is just software code. Please refer to the motivation as to why it is obvious to apply the teachings of An et al to Mikurak as is recited above.

Allowable Subject Matter

10. Claims 10 and 26-30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As per claim 10, it was not found in the prior art of a request hash table configured to maintain a mapping of certificate authority request IDs to hash values of the router requests.

As per claim 26, it was not found to be taught in the prior art of a hash value based on an enrollment message and a hash table entry mapping a pending response ID corresponding to a certificate authority pending response to the hash value.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Vaeth et al, U.S. Patent 6,308,277 discloses of ensuring that certificate transactions are certified.

Vaeth et al, U.S. Patent 6,035,402 discloses of ensuring that certificate transactions are certified.

"About Security" discloses of protocol conversion for security purposes.

Auerbach, "A Protocol Conversion Software Tool" is a general teaching of protocol conversion.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

June 13, 2004

Christopher Revak
AU 2131


6/13/04